

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

UNITED STATES OF AMERICA,)	
)	
Plaintiff,)	
)	
vs.)	Case No. 08-CR-201-TCK
)	
ANDRE RALPH HAYMOND,)	
)	
Defendant.)	

OPINION AND ORDER

Before the Court is the Order on Supervised Release (Doc. 183) (“OSR”), which alleges five violations of Defendant Andre Ralph Haymond’s (“Haymond”) conditions of supervised release: (I) violation of Mandatory Condition not to commit another federal, state or local crime - namely, possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) (“Violation I”); (II) violation of Special Computer Restriction Condition (2) requiring Haymond to disclose to the probation office all internet connection devices he possesses (“Violation II”); (III) violation of Special Condition 3(4) prohibiting Haymond from viewing or possessing any images depicting sexually explicit conduct or child pornography (“Violation III”); (IV) violation of Special Condition 3(2) authorizing the probation office to monitor all computer activity and to install remote monitoring software on all internet connections at Haymond’s expense (“Violation IV”); and (V) violation of Special Condition 1(1) requiring Haymond to attend sex offender treatment (“Violation V”).¹

On June 21, 2016, the Court conducted an evidentiary hearing on the OSR, during which Haymond contested the factual basis for all five violations. Haymond was represented by William

¹ In the OSR, there appear to be four violations due to misnumbering, but there are actually five alleged violations.

Lunn (“Lunn”), the same lawyer who represented him during his original trial and appeal. The United States presented two United States Probation Officers for the Northern District of Oklahoma as witnesses -- Sharla Belluomo (“Belluomo”) and Kory McClintock (“McClintock”). Lunn presented three witnesses -- forensic expert David Penrod (“Penrod”),² Haymond’s roommate Myra Entizne (“Myra”), and Haymond.

It is unusual for this Court to write an Opinion and Order following a revocation proceeding. However, Violation I presents complex issues and carries a mandatory minimum five-year sentence due to application of 18 U.S.C. § 3583(k). Therefore, although Violation I is being prosecuted in the form of a revocation, it has serious ramifications for Haymond, and the Court issues the following explanation of its revocation decision.

I. Factual Findings

A. Background

In 2007, when Haymond was 18 years of age, an undercover FBI agent caught Haymond sharing child pornography files on Limewire, a peer-to-peer sharing network. The FBI located Haymond’s computer, obtained a search warrant for his grandmother’s house where he resided, and seized his computer. Using a specialized software program known as Forensic Toolkit, the FBI located seventy files containing child pornography, from which they selected seven images to prosecute. These images were all of minor boys engaged in sexual activity and were part of a “Brad and Bry” series of photos known to have originated in Florida. These seven images had been deleted from Haymond’s computer, lacked metadata, and were found only in the computer’s

² Penrod was also involved in Haymond’s original trial and appeal. The Court granted funds for Penrod to travel to Tulsa and conduct his forensic examination. Penrod testified via video conference during the hearing.

“unallocated space.” After his arrest, Haymond admitted during interrogation that: (1) he was addicted to child pornography; (2) he had been accessing child pornography since 2006 using peer-to-peer file sharing programs such as Limewire; (3) he searched the Internet regularly for child pornography; (4) he deleted the images after he viewed them by reformatting his hard drive and reinstalling his Windows operating system; and (5) he was studying computer programming and video game and web design at a community college. Based on this evidence, a jury convicted Haymond of possession and attempted possession of seven images found in the unallocated space. The Court sentenced Haymond to 38 months imprisonment and 10 years supervised release, and imposed numerous conditions of release including computer monitoring.

After release from prison, Haymond commenced his term of supervised release on April 24, 2013. On April 8, 2014, Haymond was indicted in a separate case for Failure to Register as a Sex Offender. In June of 2014, he entered into an 18-month deferred prosecution agreement on that charge. While on supervised release, Haymond maintained employment. He passed several polygraph examinations inquiring whether he viewed or accessed child pornography, including one as recent as one month prior to the search and seizure leading to the current revocation. Haymond sometimes attended sex offender treatment but missed his treatment appointments on numerous occasions.

Haymond’s main problems while on supervised release related to compliance with his computer monitoring conditions. Beginning January 5, 2015, Belluomo began supervising Haymond. Belluomo testified that, from January to October of 2015, Haymond uninstalled monitoring software from his personal computer, did not stay current on his monitoring software payments, and failed to keep installation appointments with the software company. After Haymond

repeatedly failed to comply with Belluomo's directives regarding the monitoring software, Belluomo grew concerned because she could not monitor Haymond's activity on his personal computer. She gave him a strict deadline for compliance with these directives, which he did not meet. On one occasion, Haymond bragged to Belluomo that he could outsmart the monitoring software.

Based on these and other concerns, Belluomo organized a search team. On October 22, 2015, at 6:00 a.m., probation officers conducted a search of Haymond's apartment. In order to prevent deletion of illegal activity, the officers did not warn Haymond they were coming. During the search, officers seized (1) a password-protected Samsung cellular android phone belonging to Haymond ("phone"), (2) a personal computer belonging to Haymond, (3) a personal computer belonging to Haymond's roommate Myra, and (4) two other computers found in the kitchen area. Haymond had informed Belluomo of the phone and two personal computers used by himself and Myra but had not informed her of the two computers found in the kitchen area. The computers found in the kitchen were not being monitored. Although Haymond denied that these two computers were operational, he did not deny ownership of them. The phone was also not being monitored, but that had not been required by the probation office.

B. Search of Phone

1. Web History for October 21, 2015

McClintock conducted a forensic search of Haymond's phone using a Cellebrite device. Cellebrite is a mobile forensic company that provides software and devices to perform forensic examinations of mobile phones and tablets. The Cellebrite device extracts the flash memory of the phone for examination.

McClintock was only able to locate Haymond's "web history" for the day immediately preceding the surprise search, October 21, 2015. Haymond's web history for just one day indicates that he frequently uses his phone's computer to access the internet. The Court finds that Haymond daily (or at least regularly) deleted his web history but, due to the surprise search, did not have a chance to do so for October 21, 2015. The United States did not ask Haymond if, when, how, or why he cleared the web history from his phone. However, the Court takes judicial notice that clearing one's web history from a cellular phone is not a difficult task and can be a sound security practice. Therefore, while it may be relevant to avoiding detection of criminal activity, this type of deletion does not carry the same significance as wiping one's hard drive with special software and reinstalling an operating system.

On October 21, 2015, Haymond did not enter any searches for child pornography. He did enter a search for "open relationships," which the Court does not find to be a search for illicit images. Nonetheless, excluding all entries labeled "cookies" and including only those entries labeled "web history," Defendant's Exhibit 10 reveals the following relevant web history beginning at 10:09:26 PM (UTC) and ending at 10:33:39 PM (UTC):

Love TGP³
 Young Lesbians Portal [followed by: alexa004.jpg, alexa010.jpg]
 Nasty Angels - Most Charming Young Girls [followed by p02.jpg; p07.jpg; p08.jpg]
 Naked Teen Porn @ My Sexy Teens
 My Sexy Teens - Teen Pics
 18Magazine.com - 18 Magazine - Hot Teen Models Amateur & Pro
 Porn Girls Sex - Naked Girls Models, Sex Russian Style [followed by 77087.jpg]
 Naked Teens Live - Teen Nude Girl, Pictures Nude Teens [followed by 29220.jpg;
 29231.jpg]
 Teen Girls Pussy
 Teen Big Cock Pics

³ The Court finds, based on other descriptions in the web history, that TGP likely stands for teen girl porn or teen girl pussy.

Pure 18 Mobile Porn - Hot Verified 18 Years Old Teens
 Best 18 Teens - Teens Porn & Young Sex
 Teens Kitten - Teens Porn & Young Sex
 Hot Girls 4 All - free xxx galleries of sexy girls, teens
 Nubile Girls Images
 Nubile Girls Gallery, Picture 1 of 15
 Teen Girls Porn Pics
 LittleLiana.com [followed by LittleLiana.com Image#1]
 Nude Teen Pussy Young, Porn Pics
 LittleLiana.com Image #3
 LittleLiana.com Image #9
 LittleLiana.com Image #12
 Naked Pictures, Teens Nude Porn, Hardcore Young Sex
 Free Photo Porn Gallery erotic-ladies
 Young Pussy Photos and Hot Girls Porn - Fresh Teen Pics
 TeensLoveHuge Cocks presents Willow Hayes in Pussy Willow
 Real Girls - Tons of high quilty teenie's galleries
 Petite 18-19 year old teenies
 LittleLiana.com
 LittleLiana.com Image #2
 LittleLiana.com Image #4
 LittleLiana.com Image #5
 teenExtrem.com

2. Images Found in Phone's "Cache"

McClintock also located thousands of images in the cache of Haymond's phone. Of these images, McClintock testified that many of them depicted sexually explicit conduct in the form of adult pornography. She did not give a precise number, and there are no images of adult pornography in the record. McClintock also identified 59 images that depicted minors engaged in sexually explicit conduct. McClintock consulted with a member of the FBI's Internet Crime Task Force, who viewed the images and confirmed that these 59 images contained minors. These 59 images are depicted and listed in Court's Exhibit 1. In addition to the picture, this exhibit sets forth a "name" and a "path" for each image.

The 59 images in Court's Exhibit 1 can be divided into three categories based upon their path. Images 1-43 ("Browser Images") are all pornographic images portraying either young girls

engaged in various sexual acts with men or boys or close-ups of young girls' genitalia. The Browser Images contain the following path: `"/root/data/com.sec.android.app.sbrowser/cache/Cache/[number]_0_embedded_1.jpg."` Based on the evidence presented, this path indicates these particular images originated in the phone's internet browser, were not saved or downloaded to the phone, and were automatically saved to the cache.

Images 44-56 ("Gallery Images") are pornographic images containing young boys engaged in various sexual acts with men or boys. Images 45-47 contain a particular boy, and images 48, 54, and 56 contain a different particular boy. The Gallery Images contain the following path: `/Root/media/0/Android/data.com.sec.android.gallery3d/cache/imgcacheMini.0/imgcacheMini.0_embedded_[number].jpg`. The evidence is less clear as to what this path indicates, and this issue is discussed in detail below.

Images 57-59 ("APK Images") contain young girls engaged in sexual acts. The APK images contain the following path: `/Root/media/O/Download/pornvideo.apk/pornvideo.apk_embedded_1.jpg`. Based on the evidence presented, these particular images originated in the phone due to the presence of malicious "ransomware" known as Porn Droid, were not intentionally saved or downloaded to the phone, but were nonetheless saved to the cache.

All 59 images share certain characteristics. First, all images resided in the cache when the phone was searched. Penrod described the cache at issue here as a "database," or a single file or folder, that is hidden from the phone's user. McClintock testified that cache refers to the folder within the device that stores the "temporary data and cached images from websites that have been visited by whoever was using the phone." (Hrg. Tr. at 54.) Regardless of the precise meaning of the "cache" at issue in this case, the evidence is undisputed that the cache was hidden from the user,

it was impossible or difficult to access without special software such as Cellebrite or Forensic Toolkit, and Haymond did not use or have access to any such software.⁴ Evidence also shows that a user may or may not have viewed or accessed an illegal image contained in the “internet cache” when the image was previously displayed. Penrod testified:

With Internet cache databases, all that information is automatically downloaded in the background without the user’s knowledge. It’s a function of almost all Internet browsers, including this one, the Samsung browser, to download all files and data on any web page that happens to be visited. . . .

(Hrg. Tr. 101-102). This evidence is similar to that explained in *United States v. Dobbs*, 629 F.3d 1199, 1201-02 (10th Cir. 2011):

As [the expert] explained it, when a person visits a website, the web browser automatically downloads the images of the web page to the computer’s cache. The cache is populated with these images regardless of whether they are displayed on the computer’s monitor. In other words, a user does not necessarily have to see an image for it to be captured by the computer’s automatic-caching function.

Id.

Second, the images are all embedded thumbnail files, or smaller versions of a larger file. Penrod testified that, if the user clicked on a thumbnail, the full-size image would also appear in the cache. Third, the images have no metadata attached to them. This is important because metadata would perhaps allow one or more of the 59 images to be linked by date or time to a particular website visited on October 21, 2015. Without metadata, all the Court knows about the images is that they arrived in the cache file of the phone at some point prior to seizure.

⁴ In *United States v. Dobbs*, 629 F.3d 1199, 1202 (10th Cir. 2011), the expert had indicated that a “user may manipulate and control an image stored in the computer’s cache” but that Mr. Dobbs had not done so and did not know the cache existed. However, that was not the evidence presented here.

Finally, the images could not be linked to any of the sexually explicit websites Haymond visited on October 21, 2015. Penrod testified that he examined all websites, that they did not contain any of the 59 images, and they contained banners and assurances that all models were 18 years or older. The United States did not present any contrary evidence or otherwise provide any link between the 59 images in the cache and the sexually explicit websites in Haymond's web history.

II. Burden of Proof

"The burden of proof during a revocation hearing is by a preponderance of the evidence, not beyond a reasonable doubt." *Johnson v. United States*, 529 U.S. 694, 700 (2000). The Court, as the finder of fact, must be only "reasonably satisf[ied]. . . that the defendant has violated the conditions of his supervised release." *Yates v. United States*, 308 F.2d 737, 739 (10th Cir. 1962).

III. Violations II-V

The Court finds Belluomo's testimony regarding Violations II, IV, and V to be credible. Specifically, the Court finds by a preponderance of the evidence that Haymond failed to disclose the existence of two computers located in his residence (Violation II); Haymond repeatedly failed to comply with directives regarding monitoring software (Violation IV); and Haymond failed to attend numerous sex offender treatment appointments despite attempts to accommodate his schedule (Violation V). To the extent Haymond denied or offered explanations for this conduct, the Court credits Bellumo's testimony.

With respect to Violation III, Haymond's web history for October 21, 2015 proves by a preponderance of the evidence that Haymond *viewed* images depicting *sexually explicit conduct* on this date. Although Haymond did not search for sexually explicit material, there are other ways to access websites, including typing in a website address, accessing a website from favorites, or connecting to other websites through links. Haymond argues that these sites could all simply be

“redirected links” that Haymond never accessed or viewed. Haymond also argues that because “cookies” and “web history” appear in rapid succession, the “web history” could somehow be the result of “cookies.” The Court rejects these arguments as implausible. The quantity and type of web history identified above indicates that Haymond intentionally viewed sexually explicit conduct on this date. Particularly convincing to the Court are the web history entries that involve a web title or banner followed by specific images, such as Nasty Angels - Most Charming Young Girls, immediately followed by p02.jpg; p07.jpg; p08.jpg. The website names or titles indicate they are sexually explicit, and the jpg files indicate images were viewed. The Court is reasonably satisfied that Haymond viewed sexually explicit conduct on October 21, 2015 based on the web history.

In addition, as explained below, the Court concludes Haymond committed Violation I by knowingly possessing 13 images of child pornography, which is an additional factual basis for Violation III.

IV. Violation I

A. Due Process Concerns

The Court *sua sponte* makes a record on certain due process issues related to Violation I. The protections of the Due Process Clause apply to supervised release revocation hearings. *United States v. Medley*, 362 F. App’x 913, 916-17 (10th Cir. 2010). However, a defendant in a revocation proceeding is not entitled to the full panoply of rights due a criminal defendant during trial. *Id.* Federal Rule of Criminal Procedure 32.1(b)(2) outlines the limited rights afforded to a defendant during a revocation proceeding:

- (2) Revocation Hearing. Unless waived by the person, the court must hold the revocation hearing within a reasonable time in the district having jurisdiction. The person is entitled to:
 - (A) written notice of the alleged violation;
 - (B) disclosure of the evidence against the person;

- (C) an opportunity to appear, present evidence, and question any adverse witness unless the court determines that the interest of justice does not require the witness to appear;
- (D) notice of the person's right to retain counsel or to request that counsel be appointed if the person cannot obtain counsel; and
- (E) an opportunity to make a statement and present any information in mitigation.

See also Medley, 362 F. App'x at 917 (citing *Morrisey v. Brewer*, 408 U.S. 471, 488 (1972)).

Notably, a defendant is not entitled to a jury trial or the "beyond a reasonable doubt" standard.

1. Timing of Hearing

There was a considerable delay between Haymond's preliminary hearing and the revocation hearing. This delay was the result of Haymond's request for funds to hire Penrod, Penrod's review of the phone, and other steps aimed at ensuring Haymond's due process rights. Thus, Haymond waived, either actually or constructively, his right to a hearing within a reasonable time.

2. Written Notice

The OSR alleges the following:

Haymond *possessed* numerous images of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B).

(Doc. 183 at 2 (emphasis added).) During the hearing and closing arguments, counsel for the United States referenced two crimes other than possession: (1) attempted possession, which is a separate crime set forth in 18 U.S.C. § 2252(b)(2); and (2) "accessing with intent to view," which is an alternative crime in 18 U.S.C. § 2252(a)(4)(B).

With respect to written notice, the Tenth Circuit has stated:

Some circuits have required a high degree of specificity in a violations report or other form of notice about exactly which state or federal statutes have been violated, *see, e.g., United States v. Chatelain*, 360 F.3d 114 (2d Cir.2004); *United States v. Kirtley*, 5 F.3d 1110, 1113 (7th Cir.1993); *United States v. Havier*, 155 F.3d 1090 (9th Cir.1998), but no case from this circuit has required that level of specificity.

United States v. Mullane, 480 F. App'x 908, 911 (10th Cir. 2012). The Tenth Circuit held that the lower court did not commit plain error by requiring only notice that the defendant committed a Class A drug offense to be proven by evidence of drugs, scales, and cash, rather than requiring notice of the specific statute violated. *Id.* The court also noted that the defendant failed to ask for more detailed notice or time to prepare his defense. *Id.*

In this case, the problem is not the lack of notice; it is the specificity of the notice. The United States Probation Office provided notice of one specific statutory violation. The Court concludes it would violate due process to find Haymond committed the crime of attempted possession, which arises under a separate, unspecified provision. Although Haymond may not be entitled to the same type of charging specificity that he would be entitled to in an indictment, he is entitled to rely upon the fact that a specific crime alleged is the only crime he needs to defend.

With respect to “access with intent to view,” this is a closer question because it is a second type of crime alleged in the same statutory provision. Again, however, the due process problem lies in the specificity. The OSR does not merely cite § 2252(a)(4)(B); it uses the word “possession.” Possessing an image and accessing with intent to view an image are two distinct types of conduct, with different case law governing each. Because this case dealt with highly technical, forensic evidence, this is not simply a semantic difference. Haymond’s lawyer and forensic expert prepared a defense to possessing child pornography. Accordingly, the Court also finds insufficient written notice that Haymond needed to defend against “accessing with intent to view.” Again, the OSR need not contain dates, times, or other information, and it can be fairly vague and fairly broad. But in this case, the Court finds it would violate Haymond’s due process rights to revoke based on anything other than possession, given the important distinctions between possession and the two

other crimes now being discussed by the United States. Therefore, the Court limits its analysis to knowing possession.

3. 18 U.S.C. § 3853(k)

Based on the nature of Haymond's prior conviction, a finding that Haymond committed Violation I results in a minimum 5-year term of imprisonment and a 5-year to life term of supervised release. 18 U.S.C. § 3583(k). Ordinarily, revocation based on a Class A felony carries a *maximum* five-year term, still affording the revoking court discretion at sentencing. This Court is troubled by Congress's decision to permit prosecutors to elect a revocation proceeding over a criminal trial, while at the same time secure a minimum 5-year sentence and possibility of a life term on supervised release. This places the Court in a position to conduct what is in essence a criminal trial without a jury, "revoke" based merely on a preponderance of the evidence, and then be bound to a mandatory *minimum* sentence at the *maximum* sentencing range for even the most serious Class A felonies in other revocation proceedings. However, Congress passed § 3583(k), which disincentivizes prosecutors from bringing separate criminal charges (and the greater due process protections they entail) in situations such as Haymond's. *See generally* Brett M. Shockley, *Protecting Due Process from the Protect Act: The Problems with Increasing Periods of Supervised Release for Sexual Offenders*, 67 Wash. & Lee L. Rev. 353, 387 (2010) ("A prosecutor who is merely discharging her duties should almost always opt for the revocation route, because substantially less effort would be required to 'better serve the public interest' by obtaining 'the most severe penalty' available."). Thus, although the Court has serious concerns about the process authorized by Congress, the Court must proceed to analyze each element under the preponderance of the evidence standard.

B. Analysis

In relevant part, the statute provides:

(a) Any person who--

(B) **knowingly possesses . . . other matter which contain any visual depiction that . . . has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce**, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if--

(I) the producing of such visual depiction involves **the use of a minor** engaging in sexually explicit conduct; and

(ii) such visual depiction is of such conduct;

shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 2252(a)(4)(B).

1. Use of a Minor

The Court finds by a preponderance of the evidence that production of all 59 images depict minors engaging in sexually explicit conduct. This finding is based on the Court's own review of the images, McClintock's testimony regarding the images, and Haymond's failure to offer any contrary evidence or opinions. The 59 images selected by the United States Probation Office to form the basis for Violation I are not "close calls" as to the age of the child used in the depiction.

2. Knowing Possession

"[P]ossession of child pornography is an image-specific crime," meaning the United States must prove Haymond knowingly possessed at least one of the 59 particular images at issue in this case. *United States v. Haymond*, 672 F.3d 948, 954 (10th Cir. 2012). "Possession" is defined in the Tenth Circuit as holding or having something as one's own or in one's control. *Id.* at 955. At a minimum, possession requires that Haymond have the ability to "access and control" the images. *Id.* Possession can be actual -- *i.e.*, knowingly having direct physical control over the image at a

given time -- or constructive -- *i.e.*, knowingly having the power to exercise dominion or control over the image either directly or through another person. *Id.*

The Tenth Circuit has explained the “knowingly” requirement applicable to both possession and receipt of child pornography as follows:

[F]or possession of child pornography to be knowing, a defendant must know the charged images exist. As we have explained in the analogous context of knowing receipt of child pornography, defendants cannot be convicted for having the ability to control something that they do not even know exists. [*United States v.*] *Dobbs*, 629 F.3d [1199, 1207 (10th Cir. 2011)]. In other words, the defendant’s control or ability to control need[s] to relate to images that the defendant knew existed; otherwise, the defendant’s conduct with respect to the images could not be deemed to be knowing. *Id.* To convict Mr. Haymond, the government was required to prove he knew of and also controlled (or at least had the ability to access and control) the *particular* images that formed the basis of the conviction.

Id. (emphasis added).

In discussing the knowledge requirement as applied to possession charges, the Tenth Circuit in *Haymond* discussed its prior decision in *Dobbs*, wherein it reversed a jury conviction for receipt of child pornography based on the defendant’s lack of knowledge. *See Dobbs*, 629 F.3d at 1209.⁵ The *Haymond* court explained that, in *Dobbs*, there was ample evidence that the defendant had “received” the images because they ended up in the cache file of Dobbs’ computer. *Haymond*, 672 F.3d at 956. However, there was insufficient evidence to prove he received them “knowingly” because the government presented no evidence that Dobbs ever: (1) accessed the images stored in his computer’s cache; (2) knew about his computer’s automatic caching function; (3) saw the images (since a forensic expert explained that a user does not necessarily have to see an image for it to be

⁵ *Dobbs* has a vigorous dissent, 629 F.3d at 1209-18, and the majority decision has been criticized by commentators, *see, e.g., J. Elizabeth McBath, Trashing Our System of Justice? Overturning Jury Verdicts Where Evidence Is Found in the Computer’s Cache*, 39 Am. J. Crim. L. 381, 382 (2012) (criticizing *Dobbs* as too strict and ignoring evidence of past possession).

captured by the automatic caching function); or (4) controlled the images by clicking on or enlarging them. *Id.* The *Haymond* court explained that “no reasonable jury could have found [that Dobbs] knew the charged images existed on his computer or had the ability to access and control them, either when he visited the originating web pages or later, after the images had been saved to his computer’s cache.” *Id.* (emphasis added).

Applying the “knowing” definition and analysis in *Dobbs* to the facts on direct appeal in *Haymond*, the Tenth Circuit affirmed. As explained above, Haymond was originally convicted of possessing child pornography images found by FBI agents in “unallocated space” on Haymond’s computer hard drive. These charged images “somehow had been deleted and lacked metadata.” *Id.* at 952. Further, there “was no forensic evidence to show the origin of the images or how they had been deleted -- that is, whether by the user or by the computer’s automated processes with no prompting at all from the user.” *Id.* at 952-53. However, Haymond had admitted during interviews that “he had been downloading child pornography [from Limewire] once or twice every month or two, and that after downloading the files, he would clean the registry, reformat his computer’s hard drive, and reinstall his Windows operating system.” *Id.*

The Tenth Circuit found Haymond knowingly possessed the charged images, highlighting factual distinctions between Dobbs’ knowledge and Haymond’s knowledge:

In this case, unlike in *Dobbs*, there was ample evidence from which a reasonable jury could infer Mr. Haymond knew the charged images were on his computer because he searched for and then downloaded them from LimeWire. Here, Mr. Haymond admitted to frequently searching for and downloading child pornography from LimeWire. Mr. Carter testified he found the LimeWire program on Mr. Haymond’s computer. The government also introduced three images of child pornography that Agent Whisman found in Mr. Haymond’s shared LimeWire folder, which the district court permitted the jury to consider as “proof of ... [the] absence of mistake,” Fed.R.Evid. 404(b), a ruling that is not challenged on appeal. The jury was not required to credit Mr. Haymond’s assertions that he inadvertently downloaded child pornography from LimeWire while attempting to obtain music, particularly when he

had admitted he was addicted to child pornography and used LimeWire to search for and download it. *It was thus permissible for the jury to infer that Mr. Haymond used LimeWire exclusively to search for and download child pornography.* Viewing the evidence in the light most favorable to the verdict, we conclude it was sufficient to permit a rational jury to find beyond a reasonable doubt that *Mr. Haymond knew the charged images were on his computer once he deliberately selected and downloaded them from LimeWire.*

Id. (emphasis added). Although Penrod had testified that the images “were thumbnails which came from web pages and could not have come from Limewire,” the FBI agent testified it “was not possible to determine whether the images were thumbnails.” *Id.* at 956 n.15. Thus, a jury could infer that Haymond “used Limewire exclusively to search for and download child pornography.” *Id.* at 956. This inference was critical because there was nothing linking the seven charged images with any particular Limewire search. In order for the knowledge to be “image specific,” therefore, the jury had to plausibly infer that *all* child pornography in Haymond’s unallocated space originated exclusively from Limewire downloads rather than an internet browser.

As to Haymond’s ability to exercise control over the seven charged images, the court reasoned:

Unlike the defendant in *Dobbs*, who sought out child pornography on internet websites, Mr. Haymond admitted to seeking out and downloading child pornography through peer-to-peer programs, including LimeWire. As the defense’s own forensic specialists testified, downloading from LimeWire does not occur automatically. It requires the user to highlight the names of the file or files he wishes to download and then to press “enter.” In contrast to the caching process at issue in *Dobbs*, which occurs automatically, this type of volitional downloading entails “control” sufficient to establish actual possession. Accordingly, the evidence here was sufficient to permit a reasonable jury to conclude beyond a reasonable doubt that Mr. Haymond “knowingly possessed” the charged images.

Id. at 956-57. Yet again, important information is contained in a footnote:

Because we conclude there was sufficient evidence to establish Mr. Haymond knowingly possessed the images by downloading them, we need not decide whether he constructively or actually possessed the charged images after they were deleted and resided in his computer’s unallocated space. As a result, *United States v. Flyer*,

633 F.3d 911 (9th Cir. 2011), which held the defendant could not “knowingly possess” child pornography *once it had reached his computer’s unallocated space*, is inapposite. Nor do we decide whether, as the government claims, Mr. Haymond’s admissions were sufficient to prove he exercised control over those particular images by deleting them.

Id. at 957 n.16 (emphasis added). This footnote indicates that the Tenth Circuit affirmed Haymond’s conviction on a theory of Haymond’s knowing possession in the past. Specifically, Haymond had knowingly possessed the seven images at a previous time when he downloaded them from Limewire, although they existed only in unallocated space when his computer was searched. The court did not reach two other questions: (1) whether he possessed them in the unallocated space, in light of admissions and other circumstantial evidence; and (2) whether his deletion of the charged images was sufficient to prove past possession.

Applying the hearing evidence in this case to the legal principles articulated in *Haymond* and *Dobbs* is not a straight-forward task. Commentators have struggled with questions similar to those presented here. *See generally McBath*, 39 Am. J. Crim. L. at 382, *supra* note 5; Katie Gant, *Crying over the Cache: Why Technology Has Compromised the Uniform Application of Child Pornography Laws*, 81 Fordham L. Rev. 319, 322 (2012) (analyzing what “knowingly” means “in a technologically advanced day and age”). When encouraged to do so by the Court at the close of evidence, the United States declined to offer additional briefing setting forth the law in conjunction with the hearing evidence. Thus, the legal arguments in Haymond’s brief stand largely un rebutted.⁶

a. Browser Images/APK Images

⁶ Rather than offer briefing, the United States simply argued that *Dobbs* does not apply to possession cases because it was a receipt case. Even a cursory reading of *Haymond*, however, reveals that the Tenth Circuit views *Dobbs*’ “knowing receipt” analysis as highly relevant to “knowing possession.”

The United States failed to prove by a preponderance of the evidence that Haymond knowingly possessed the Browser Images or the APK Images. The Court finds insufficient evidence to show that Haymond, while on supervised release, either: (1) conducted searches related to these images or other child pornography; (2) accessed websites containing these images or other child pornography; (3) downloaded these images from a peer-to-peer network or the internet; (4) clicked on or enlarged these images while they were in the browser or the cache; (5) attempted to delete these images from the cache; or (6) used any “washing” software in attempt to delete these images from the cache.

With respect to the Browser Images, the United States must do more than merely show the images were in the cache file of a phone possessed and controlled by Haymond. This is because, under Tenth Circuit law explained above, a user does not necessarily view, access, or control images that are automatically cached from an internet browser. In this case, in contrast to Haymond’s original case, the evidence of any searching or volitional acts related to the Browser Images is wholly lacking. With respect to the APK Images, they arrived in the cache via malicious software known as Porn Droid. Penrod’s testimony indicates that a user does not necessarily view, access, or control images from this type of malicious software, and there is no evidence that Haymond possessed or took any volitional acts whatsoever related to those images. Accordingly, the United States has failed to show Haymond knowingly accessed, controlled, or otherwise possessed the Browser Images or the APK Images (1) at any point in time prior to the search of his phone, or (2) at the time the phone was searched. The majority’s reasoning in *Dobbs*, as explained and amplified in *Haymond*, is directly on point with respect to the Browser Images and APK Images.

b. Gallery Images

For the same reasons explained above, the United States failed to prove knowing possession of the Gallery Images based merely on their existence in the cache at the time Haymond's phone was searched. However, the Gallery Images pose a more difficult question on the issue of past possession, *i.e.*, whether Haymond knowingly possessed the Gallery Images at a point in time prior to search. The crucial technical question is whether the "3d gallery" designation in the path tends to show Haymond exercised control over the images at a previous point in time. If the path tends to prove Haymond saved or had access to the images in an application on his phone, this is a crucial distinction from the Browser Images and APK Images.

Curiously, the United States did not highlight the different path or separately discuss the Gallery Images during its case in chief. Instead, this distinction was elicited during Penrod's testimony. The critical testimony relied upon by the Court in reaching its decision is set forth below:

[Cross-Examination by United States]

- Q. So, going back to prior when you talked about the 59 images appearing from the S browser cache file, not only do we have the pornvideo app as a source of three of the images, but we have the Gallery 3D, the photo viewing app, as responsible for 13 of the images; is that correct?
- A. Correct.
- Q. And your rationale with respect to how the website loads and the items that are not visible at the bottom of the web page, that's not applicable to Gallery 3D because it's not a website; right?
- A. Yeah, it functions in the same way. It's simply a cache of thumbnails that are created through Gallery in almost the exact same method or process.
- Q. Okay. So when you were talking about being unable to potentially see items that were in the cached file, you were talking about the Samsung browser; is that right?
- A. That's right.
- Q. Okay. Now, you would agree with me that it doesn't take a -- that 99.9 percent of users that have an Android phone and have Gallery 3D, that they can, without special software, navigate to their photo gallery?
- A. Correct, yes.
- Q. And within this piece of the phone that is accessible to your average user, an app that comes stock or is an easily downloadable app for Samsung users, they have the ability to look at photos through the Gallery 3D application?

A. That's correct.

Q. And --

A. Through Gallery.

Q. Through Gallery?

A. The Gallery, right.

Q. *So a cached file from the Gallery indicates that, just the same way as for the Samsung browser, that at one point an image that corresponded to that cached file was present in that application?*

A. Correct.

...

[Redirect by Lunn]

Q. Now, how is it that a person would not know about the images that are in the Android gallery if they wound up in his cache?

A. *Well, the gallery cache functions in the same way that the browser cache does: it's a cached database and it contains thumbnails. If your phone has a large number of images on it, that all those images are going to be represented, once Gallery finds them, they'll be represented in the Gallery 3D cache folder, cache database.*

Q. And Mr. Haymond's phone had a large number of images on it; is that a fair statement?

A. Yes.

Q. We're talking about tens of thousands of images; is that right?

A. Yes, that's correct.

Q. So, the fact that something is in the -- coming from the Android Gallery doesn't necessarily mean that he has gone down and looked at every single one of those 10-, 20-, 30,000 images?

A. Well, a significant number of those images are images that are in cache, they're spread out through the -- they're part of various programs, for example, *so those types of files would not end up in Gallery 3D. Just it's going to go out and look for actual images throughout the phone.*

Q. Now then, and so it's possible under those circumstances that somebody can actually have a -- can get something in their computer cache from the Android Gallery and not know about those images?

A. *Yeah, that's absolutely true because the Gallery 3D cache database contains images from all over the phone, not just from one particular folder on the phone, but from all over the phone.*

...

[Re-Cross by United States]

- Q. You testified on cross-examination, and then again on redirect examination, that the way the gallery works is it searches the phone for what images may be available on the phone; correct?
- A. Correct.
- Q. Gallery doesn't search the Internet for what might be available in the universe of images on the Internet?
- A. No.
- Q. So Gallery is only going to aggregate or show you the photo depictions of items on your phone?
- A. Correct.
- Q. And Mr. Lunn's question to you was that it was possible to have these in your gallery and not know they were there. I believe he asked you that question. Do you recall?
- A. Yes.
- Q. But in this case there's not an explanation that's similar to the Samsung browser that explains how they got there; is that correct?
- A. That's correct, yes.
- Q. So you said before on direct examination that there is no evidence on the phone that somebody clicked on or enlarged a photo or moved a photo between folders. But if the person were to acquire the suspected images from the Internet, its presence in the Gallery would indicate a movement of sorts, that it moved from just being something available on a web page to actually being on the phone?
- A. Well, again, the rules for this cache are just like the cache in the web browsers; there's nothing here that tells you anything about these images. It's not telling you how, when, where they were other than the fact that they're inside this cache.
- Q. *So, Mr. Penrod, Gallery shows the images that are on the phone?*
- A. *Correct.*
- Q. *Not what's on the Internet, not what's potentially available, but what's actually on the phone?*
- A. *That's correct.*
- Q. *And what we know, without knowing where on the phone it was located, is that somehow it got onto the phone?*
- A. *Correct.*

(Hrg. Tr. 131:22-133:7; 136:25-138:6; 141:6-142:20 (emphases added).)

Based on this testimony and other circumstantial evidence, the Court concludes it is more likely than not that Haymond knowingly possessed the Gallery Images at a point in time prior to search of the phone. First, the Court finds Haymond had nearly exclusive use and possession of his

password-protected phone and rejects any argument that someone other than Haymond possessed the phone at relevant times.

Second, the Court finds that only those images actually “on the phone” (and not images merely accessed or viewed on the phone using a browser application) would have a “gallery 3d” path when found in the cache. The Court interprets “on the phone” to mean saved, downloaded, or otherwise accessible on the phone in some application for viewing at the user’s discretion. The Court recognizes that Penrod’s testimony is not perfectly clear on this point, particularly during re-cross. However, based on careful examination of his testimony as a whole, the Court finds by a preponderance of the evidence that Haymond knowingly took some volitional act related to the Gallery Images that resulted in the images being on his phone in a manner consistent with knowing possession. Although the images were no longer in an accessible area of the phone at the time of the search, the path convinces the Court that these 13 images previously resided in an accessible area of Haymond’s phone and were under his control. This is distinct from the Browser Images, which, under the Tenth Circuit’s reasoning in *Haymond* and *Dobbs*, were not necessarily saved, downloaded, viewed, accessed, or controlled in any manner prior to residing in the cache. This is also distinct from the APK Images, which arrived to the phone via malicious software.

Third, the path demonstrates that Haymond took prior volitional actions with regard to the Gallery Images. In *Haymond*, the Tenth Circuit reasoned that volitional downloads from Limewire provided evidence that Haymond knowingly possessed the images prior to their arrival in the “unallocated space” of his computer. Saving, downloading, or otherwise placing the image in an application on the phone is a similar volitional act. Further, the evidentiary link between Haymond’s prior volitional act(s) and the Gallery Images found in the cache is even greater than that present between Haymond’s Limewire downloads and the “Brad and Bry” images found in the

unallocated space. In order for there to be an image-specific link to the Brad and Bry images, the jury had to conclude all images in the unallocated space necessarily originated as Limewire downloads. Here, based on the path, there is stronger evidence that each of the 13 Gallery Images were once knowingly possessed by Haymond.

Finally, although the United States failed to highlight this key fact, the 13 Gallery Images depict sexual acts between young boys or between boys and adult males. Viewing the 59 images as a whole, these 13 images stand out as distinct from the Browser Images and the APK Images and are more consistent with images forming the basis of Haymond's original conviction. Therefore, the content of these 13 images contributes to this Court's finding of knowing possession of the Gallery Images.

3. Interstate Commerce

For the Gallery Images, the next question is whether the United States met its burden of proving, by a preponderance of the evidence, that the digital images "contain any visual depiction . . . that has been . . . transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce . . . by any means including by computer[.]" 28 U.S.C. § 2252(a)(4)(B). This language, which was revised by the Effective Child Pornography Prosecution Act of 2007 ("ECPPA"), Pub. L. No. 110-358, § 102(7), 122 Stat. 4001 (2008), represents an expansion of the statutory language governing Haymond's original conviction.⁷

The ECPPA was a direct response to the Tenth Circuit's decision in *United States v. Schaefer*, 501 F.3d 1197 (10th Cir. 2007), which held that use of the Internet alone did not confer

⁷ On appeal, the Tenth Circuit affirmed the interstate commerce element based on an FBI agent's testimony that the "Brad and Bry" images were originally taken in Florida and had necessarily crossed state lines at some time before reaching Haymond's computer in Oklahoma. *See Haymond*, 672 F.3d at 954. Much less evidence is required under the current statute.

federal jurisdiction. *See* Jonathan R. Gray, *United States v. Schaefer and United States v. Sturm: Why the Federal Government Should Regulate All Internet Use As Interstate Commerce*, 90 Denv. U. L. Rev. 691, 709 (2012) (“In direct response to *Schaefer*, Congress expressed its intent that ‘transmission of child pornography using the Internet constitutes transportation in interstate commerce.’”) (quoting public law). By adding “any means or facility of interstate commerce” and “in or affecting interstate commerce,” Congress “made it clear to the courts that it intended the statute to reach the full extent of Congress’s Commerce Clause power” and “answered the call from the Tenth Circuit in *Schaefer* demanding more precise language.” *Id.* This expanded language has withstood constitutional challenges under the Commerce Clause. *See e.g., United States v. Konn*, 634 F. App’x 818, 821 (2d Cir. 2015) (rejecting argument that ECPA exceeded Congress’s commerce power because “there can be no question that the Internet is a channel and instrumentality of interstate commerce; and Congress may regulate and protect the instrumentalities of interstate commerce”).

Under this relaxed standard, the United States need only show that it is more likely than not that the Gallery Images arrived on Haymond’s phone from use of the internet, rather than some other means such as Haymond taking the photos himself. The Court is reasonably satisfied these images, which are thumbnails, were originally saved or downloaded to Haymond’s phone from the internet.

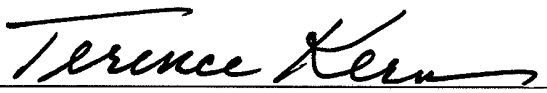
V. Conclusion

The United States failed to call its own forensic expert, failed to assist the Court in applying Tenth Circuit law on “knowing possession” to its evidence, and failed to prove Haymond knowingly possessed any of the 59 images beyond a reasonable doubt. If this were a criminal trial and the Court were the jury, the United States would have lost. This highlights the Court’s concerns with § 3583(k) and the mandatory penalties it carries. Nonetheless, for reasons explained above, the

Court finds it is more likely than not that Haymond knowingly possessed, accessed, controlled, and viewed the thirteen Gallery Images at some time prior to search of his phone, in violation of 18 U.S.C. § 2252(a)(4)(B).

Accordingly, the Court hereby revokes Haymond's term of supervised release based on a finding that he committed Violations I-V. The United States Probation Office is ordered to prepare a Presentence Investigation Report. Sentencing is set for Friday, September 16, 2016, at 11:00 a.m.

DATED THIS 2nd day of August, 2016.


TERENCE KERN
United States District Judge